HISTÓRICO DE REVISÕES

REVISÃO	DATA REV.	ALTERAÇÕES
005	21/01/2016	Alteração do item 1, contemplando os objetivos do documento, não do SGSI; Item 5.4 – revisão das regulamentações.

ÍNDICE

1. OBJETIVO

Esta política de segurança tem por objetivo a definição de diretrizes para proteção estratégica do negócio de certificação digital e dos ativos de informação da Certisign, contra ameaças internas ou externas, deliberadas ou acidentais.

2. RESPONSABILIDADES

2.1. Alta Direção da Certisign

A Alta Direção da Certisign compromete-se com esta política, apoiando as metas e princípios da segurança da informação, alinhada com os objetivos e estratégias do negócio.

2.2. Gerencia de Segurança da Informação

A Gerencia de Segurança da Informação é responsável por manter a política, prover suporte e aconselhamento durante a sua implementação e vigência.

2.3. Gerentes

Todos os gestores são diretamente responsáveis pelo cumprimento desta política, estendendo esta responsabilidade a toda sua equipe.

2.4. Usuários da Informação

É mandatório o cumprimento desta política por todos os usuários da informação (funcionários, terceiros, consultores e fornecedores) da Certisign. O seu descumprimento implicará na aplicação de sanções previstas na legislação e regulamentos vigentes.

3. REFERÊNCIAS

REF.	NOME DO DOCUMENTO	CÓDIGO
1	Política de Segurança da ICP-Brasil - DOC-ICP-02	EXT-DOC-ICP-0002
2	Requisitos Mínimos para as declarações de Práticas de Certificação das Autoridades Certificadoras da ICP-Brasil - DOC-ICP-05	EXT-DOC-ICP-0005
3	Security and Audit Requirements - SAR	EXT-GUI-VRS-0001
4	ABNT NBR ISO/IEC 27001:2013 – Tecnologia da Informação – Técnicas de Segurança – Sistema de Gestão da Segurança da Informação. Item 5.2 e Anexo A.5.1.1 e 5.1.2	EXT-NRM-ABN-0002
5	ABNT NBR ISO/IEC 27002:2013 – Tecnologia da Informação – Técnicas de Segurança – Código de prática para controles de Segurança da Informação.	EXT-NRM-ABN-0003

4. DEFINIÇÕES

4.1. Confidencialidade

Características das informações que estão disponíveis somente para pessoas autorizadas ou sistemas.

4.2. Integridade

Características das informações que somente são alteradas somente por pessoas da forma permitida.

4.3. Disponibilidade

Características das informações que somente pode ser acessada por pessoas autorizadas quando for necessário.

4.4. Segurança da informação

Preservação da confidencialidade, integridade e disponibilidade da informação.

4.5. Sistema de gestão da segurança da informação

Sistema de gestão que cuida do planejamento, implementação, manutenção, revisão e aprimoramento da segurança da informação.

4.6. Comitê do SGSI

Comitê criado para ajudar no processo de Gestão do Sistema de Segurança da Informação, de forma direta e operacional.

4.7. Incidente de Segurança

Um ou uma série de eventos de Segurança da Informação indesejados ou inesperados, relacionados a segurança de sistemas de computação ou de redes de computadores.

4.8. Plano de Continuidade da Segurança da Informação.

Conjunto de estratégias e planos de ação criados para garantir que os serviços essenciais sejam devidamente identificados e preservados após a ocorrência de um desastre.

5. REGULAMENTAÇÕES

5.1. Confidencialidade

- Os Sistemas corporativos e de informações da Certisign devem ser acessados somente por pessoas autorizadas;

5.2. Integridade

- A integridade das informações deve ser protegida contra utilização e/ou modificação não autorizada;

5.3. Disponibilidade

- As informações para os processos de negócio devem estar sempre disponíveis;

5.4. Regulamentação

- Os requisitos legais e regulatórios devem ser cumpridos e auditados;
- A gestão dos funcionários devem obedecer obrigatoriamente os requisitos legais e de uma Autoridade Certificadora;
- Os requisitos internos, contratuais e estatutários devem ser cumpridos por todos.

5.5. Responsabilidade

- O Comitê do SGSI formado com as áreas críticas do negócio deve garantir a segurança e a continuidade dos serviços;

5.6. Inventário de Ativos

- Os inventários de ativos devem ser atualizados periodicamente armazenados em local seguro;

5.7. Classificação da Informação

- Todos os documentos, procedimentos e qualquer informação documentada devem ser classificados e rotulados de acordo com a Política de Classificação da Informação;

5.8. Avaliação de Riscos

- Todos os Ativos devem ser avaliados periodicamente e dever ter determinados seus riscos ao negócio da Certisign;

5.9. Tratamento de Riscos

- Todos os riscos e ameaças à segurança da informação devem ser tratados através da implementação de controles devem ser reavaliados periodicamente;

5.10. Aceitação de Riscos

- Os riscos residuais à segurança da informação devem ser aprovados pela Alta Direção e devem ser reavaliados periodicamente;

5.11. Treinamento e Conscientização

- Todos os usuários das informações devem ser treinados e conscientizados quanto às diretrizes de segurança da informação da Certisign;

5.12. Operação

- A operação do sistema e da infraestrutura responsável pelo ciclo de vida da certificação digital deve garantir a operação segura e correta dos recursos de processamento da informação, através de processos seguros e que garantam a geração de trilhas dos eventos.

5.13. Monitoramento

- Todos os processos devem ser monitorados para avaliação do desempenho da segurança da informação;

5.14. Tratamento de Incidentes

- Os incidentes de Segurança ocorridos na Certisign devem ser reportados para a Gerência de Segurança, principalmente os casos de indisponibilidade de sistemas e vazamento de informação de clientes;

5.15. Continuidade da segurança da informação

- O plano de continuidade da segurança da informação deve ser mantido atualizado e validado;

5.16. Auditorias

- As realizações periódicas das auditorias devem verificar a eficácia do SGSI e de seus controles, bem como se está efetivamente implementado e mantido;

5.17. Análise Crítica da Política de SI

- Anualmente ou sempre que surgir uma mudança significativa no modelo de negócio deve ser realizado um processo formal de análise crítica da Política de Segurança;

5.18. Melhoria Contínua

- A Certisign deve continuamente monitorar, medir, analisar, avaliar, ajustar e implementar melhorias buscando a eficácia do Sistema de Gestão de Segurança da Informação.

Esta política é suportada por um conjunto de processos, práticas, manuais e procedimentos.

6. ANEXOS

REF.	NOME DO DOCUMENTO	CÓDIGO
[Nº SEQUENCIAL]	[TÍTULO DO DOCUMENTO]	[CODIFICAÇÃO EXISTENTE]